

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representation of  
The original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

Requested Patent JP8328470

Title:

KEY FORMING SYSTEM FOR DIGITAL SIGNATURE AND IC CARD FOR MAKING  
SIGNATURE BY USING THE KEY

Abstracted Patent: JP8328470

Publication Date: 1996-12-13

Inventor(s): IEGI TOSHIATSU

Applicant(s): N T T DATA TSUSHIN KK

Application Number: JP19950156799 19950531

Priority Number(s):

IPC Classification: G09C1/00 ; G06K17/00 ; H04L9/32

Equivalents:

ABSTRACT:

PURPOSE: To make it possible to rapidly form signature forming keys for many persons with a digital signature system.

CONSTITUTION: Just one pair of two pieces of prime numbers P1, Q1 of a large number of digits of about decimal 100 digits are formed for N persons in a key formation center 1. A pair of a cipher key E1 and a decryption key D1 are formed in accordance with therewith and N pieces of card identifiers IDj (j=1 to N) of different values are formed. The common decryption key D1 is stored as a secret key in the respective non-rewritable and non-externally readable memory areas of N sheets of IC cards 2-j (j=1 to N). The individual card identifiers IDj are otherwise stored in the non-rewritable memory areas 23. The digital signature is formed by adding the card identifiers IDj to objective information, then ciphering the set of the objective information and the card identifiers IDj with the decryption key D1 in the case the digital signature is executed by using such IC card 2-j.

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-328470

(43)公開日 平成8年(1996)12月13日

(51)Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 9 C 1/00		7259-5 J	G 0 9 C 1/00	
G 0 6 K 17/00			G 0 6 K 17/00	V
H 0 4 L 9/32			H 0 4 L 9/00	A

審査請求 未請求 請求項の数 8 F D (全 7 頁)

(21)出願番号 特願平7-156799

(22)出願日 平成7年(1995)5月31日

(71)出願人 000102728

エヌ・ティ・ティ・データ通信株式会社  
東京都江東区豊洲三丁目3番3号

(72)発明者 家木 俊温

東京都江東区豊洲三丁目3番3号 エヌ・  
ティ・ティ・データ通信株式会社内

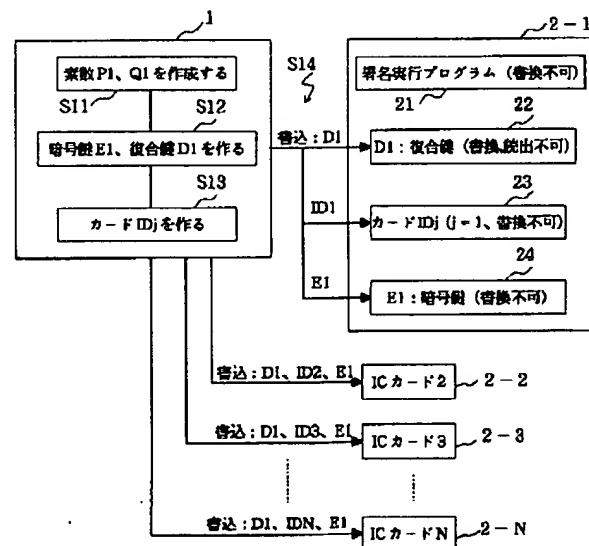
(74)代理人 弁理士 上村 輝之

(54)【発明の名称】 デジタル署名のための鍵生成方式及びその鍵を用いて署名を行う I C カード

(57)【要約】

【目的】 デジタル署名システムにおいて、多数の人数分の署名作成用鍵を短時間で生成できるようにする。

【構成】 鍵生成センタ 1 において、N 人の者に対して、10 進 100 桁程度の大桁数の 2 個の素数 P1、Q1 を 1 対だけ作成し、これに基づいて 1 対の暗号鍵 E1 と復号鍵 D1 を生成すると共に、異なる値の N 個のカード識別子 IDj (j = 1 ~ N) を生成する。そして、N 枚の I C カード 2-j (j = 1 ~ N) の各々の、書換え不可・外部読み出し不可の記憶エリア 22 に秘密鍵として共通の復号鍵 D1 を格納し、また、書き換え不可の記憶エリア 23 に個別のカード識別子 IDj を格納する。この I C カード 2-j を用いてデジタル署名を行う場合、対象情報にカード識別子 IDj を付加した上で、この対象情報とカード識別子 IDj のセットを復号鍵 D1 で暗号化することによりデジタル署名を作成する。



1

## 【特許請求の範囲】

【請求項1】 デジタル署名のための秘密の復号鍵及び公開の暗号鍵を生成する方式において、複数署名者に対し、共通な1対の素数に基づいて共通の1対の復号鍵及び暗号鍵を作成する共通鍵作成手段と、前記複数署名者に対し、各人毎に異なる個別の識別子を作成する個別識別子作成手段と、前記複数署名者に配付されるべき複数枚のICカードの各々に、前記共通の復号鍵と前記個別の識別子とを書込む鍵書込み手段とを備えたことを特徴とするデジタル署名のための鍵作成方式。

【請求項2】 前記鍵書込み手段が、各ICカードの書き換え不可かつ外部読み出し不可の記憶エリアに前記共通の復号鍵を書込み、書き換え不可の記憶エリアに前記個別の識別子を書込むことを特徴とする請求項1記載のデジタル署名のための鍵作成方式。

【請求項3】 デジタル署名のための秘密の復号鍵及び公開の暗号鍵を生成する方式において、複数署名者に対し、桁数の比較的多い共通の1対の素数に基づいて共通の1対の復号鍵及び暗号鍵を作成する共通鍵作成手段と、前記複数署名者に対し、桁数が比較的小なく且つ各人毎に異なる個別の複数対の素数に基づいて個別の複数対の復号鍵及び暗号鍵を作成する個別鍵作成手段と、前記複数署名者に配付されるべき複数枚のICカードの各々に、前記共通の復号鍵と前記個別の復号鍵とを書込む鍵書込み手段とを備えたことを特徴とするデジタル署名のための鍵作成方式。

【請求項4】 前記鍵書込み手段が、各ICカードの書き換え不可かつ外部読み出し不可の記憶エリアに前記共通の復号鍵及び前記個別の復号鍵を書込むことを特徴とする請求項1記載の鍵作成方式。

【請求項5】 デジタル署名のための秘密の復号鍵及び公開の暗号鍵を生成する方法において、複数署名者に対し、共通な1対の素数に基づいて共通の1対の復号鍵及び暗号鍵を作成する共通鍵作成過程と、前記複数署名者に対し、各人毎に異なる個別の識別子を作成する個別識別子作成過程と、前記複数署名者に配付されるべき複数枚のICカードの各々に、前記共通の復号鍵と前記個別の識別子とを書込む鍵書込み過程とを備えたことを特徴とするデジタル署名のための鍵作成方法。

【請求項6】 デジタル署名のための秘密の復号鍵及び公開の暗号鍵を生成する方法において、複数署名者に対し、桁数の比較的多い共通の1対の素数に基づいて共通の1対の復号鍵及び暗号鍵を作成する共通鍵作成過程と、前記複数署名者に対し、桁数が比較的小なく且つ各人毎に異なる個別の複数対の素数に基づいて個別の複数対の復号鍵及び暗号鍵を作成する個別鍵作成過程と、

2

前記複数署名者に配付されるべき複数枚のICカードの各々に、前記共通の復号鍵と前記個別の復号鍵とを書込む鍵書込み過程とを備えたことを特徴とするデジタル署名のための鍵作成方法。

【請求項7】 記憶している秘密の復号鍵を用いてデジタル署名を作成するICカードにおいて、前記復号鍵を記憶するための書き換え不可かつ外部読出し不可の記憶エリアと、

当該ICカードの識別子を記憶するための書き換え不可の記憶エリアと、

対象情報に前記識別子を付加した上で、この対象情報と識別子のセットを前記復号鍵を用いて暗号化することによりデジタル署名を作成する署名作成手段と、を備えたことを特徴とするICカード。

【請求項8】 記憶している秘密の復号鍵を用いてデジタル署名を作成するICカードにおいて、

第1の復号鍵及び第2の復号鍵を記憶するための書き換え不可かつ外部読出し不可の記憶エリアと、

対象情報を前記第1の復号鍵を用いて暗号化することにより第1のデジタル署名を作成して、前記対象情報に付加した上で、この対象情報と第1の復号鍵とのセットを前記第2の復号鍵を用いて暗号化することにより第2のデジタル署名を作成する署名作成手段と、を備えたことを特徴とするICカード。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明は、例えば署名入りの金融取引証明書に用いられる署名や、ネットワークアクセス者の署名等を電子的に作成するデジタル署名に関わり、特にデジタル署名に用いる鍵の生成方式及びその鍵を用いて署名を行うためのICカードに関する。

## 【0002】

【従来の技術】 近年、通信や金融取引等の分野においては、ある事実を証明する手段として電子的に署名を行うデジタル署名の重要性が急速に増大している。この場合、これらのシステムが大規模なことから、不特定多数の人間の誰の署名であるかを特定することが必要となる。

【0003】 RSA (Rivest-Shamir-Adleman) 暗号を署名関数として用い、秘密鍵をICカードに格納する電子署名方式が知られている(特開平4-118777)。一般に、RSA暗号を用いる署名方法では、周知のように、大きな2つの素数P、Qが予め選ばれ、これに基づいて規定の方法で暗号鍵と復号鍵とが作成される。

【0004】 図6は、この従来のデジタル署名作成方法を示す。鍵生成センタでは、N人の顧客に対し、2個の素数P<sub>i</sub>、Q<sub>i</sub> (i=1~N)の対をN対作成し(ステップS1)、N対の暗号鍵E<sub>i</sub>と復号鍵D<sub>i</sub>を作成する(ステップS2)。そして、この暗号鍵E<sub>i</sub>と復号鍵D<sub>i</sub>

3

1をそれぞれ公開鍵(=検証鍵)、秘密鍵(=署名鍵)としてN枚のICカード1~Nにそれぞれ書き込み、各ICカード1~Nを各顧客に渡す。各顧客は、そのICカードを用いて取引文を復号鍵D1(=秘密鍵)で暗号化することにより、その取引文にデジタル署名を行う。署名された取引文は取引相手に送られ、そこで暗号鍵E1(=公開鍵)を用いて復号化されることにより、正しく署名されたものか否かが検証される。

【0005】

【発明が解決しようとする課題】上記従来のデジタル署名作成方法では、RSA暗号で必要な強度を保つため、素数P1、Q1として、10進100桁程度の極めて大きい数を用いる必要がある。そのため、1対の暗号鍵E1及び復号鍵D1を作成するために、一般に数分程度の時間がかかる。従って、多数の人数分の鍵を作成する場合には膨大な時間を必要とし、実現性に乏しいという問題点がある。

【0006】本発明は上記従来の問題点に鑑み、多数の人数分の鍵を短時間で作成することができるデジタル署名用鍵の生成方式を提供することを目的とする。

【0007】また、本発明の別の目的は、そのように作成された鍵を用いて安全性の高いデジタル署名を作成することのできるICカードを提供することにある。

【0008】

【課題を解決するための手段】本発明の第1の側面に従うデジタル署名用鍵の生成方式は、複数人の署名者に対し、共通な1対の素数に基づいて共通の1対の復号鍵及び暗号鍵を作成する共通鍵作成手段と、上記複数署名者に対し、各人毎に異なる個別の識別子を作成する個別識別子作成手段と、上記複数署名者に配付されるべき複数枚のICカードの各々に、上記共通の復号鍵と上記個別の識別子とを書込む鍵書き込み手段とを備えたことを特徴とする。

【0009】この方式において、望ましくは、ICカードの書換え不可かつ外部読み出し不可の記憶エリアに上記共通の復号鍵が書込まれ、書換え不可の記憶エリアに上記個別の識別子が書込まれる。

【0010】本発明の第2の側面に従う鍵生成方式は、複数署名者に対し、桁数の比較的多い共通の1対の素数に基づいて共通の1対の復号鍵及び暗号鍵を作成する共通鍵作成手段と、上記複数署名者に対し、桁数が比較的小なく且つ各人毎に異なる個別の複数対の素数に基づいて個別の複数対の復号鍵及び暗号鍵を作成する個別鍵作成手段と、上記複数署名者に配付されるべき複数枚のICカードの各々に、上記共通の復号鍵と個別の復号鍵とを書込む鍵書き込み手段とを備えたことを特徴とする。

【0011】この方式では、望ましくは、ICカードの書換え不可かつ外部読み出し不可の記憶エリアに上記共通の復号鍵及び個別の復号鍵が書込まれる。

【0012】本発明の第3の側面に従うデジタル署名用

4

のICカードは、秘密鍵たる復号鍵を記憶するための書き換え不可かつ外部読出し不可の記憶エリアと、当該ICカードの識別子を記憶するための書き換え不可の記憶エリアと、対象情報に上記識別子を付加した上で、この対象情報と識別子のセットを上記復号鍵を用いて暗号化することによりデジタル署名を作成する署名作成手段とを備えたことを特徴とする。

【0013】本発明の第4の側面に従うデジタル署名用のICカードは、秘密鍵たる第1の復号鍵及び第2の復号鍵を記憶するための書き換え不可かつ外部読出し不可の記憶エリアと、対象情報を第1の復号鍵を用いて暗号化することにより第1のデジタル署名を作成して、これを対象情報に付加した上で、この対象情報と第1の復号鍵とのセットを第2の復号鍵を用いて暗号化することにより第2のデジタル署名を作成する署名作成手段とを備えたことを特徴とする。

【0014】

【作用】本発明の第1又は第2の側面に従う鍵生成方式では、複数人の署名者に対し、共通の1対の素数に基づいて共通の暗号鍵及び復号鍵を作成し、また、各人毎に異なる個別の識別子又は個別の暗号鍵及び復号鍵を作成し、この共通の復号鍵(秘密鍵)と個別の識別子又は個別の復号鍵(秘密鍵)とを各人のICカードに書込む。この作成方式によれば、複数人に対して共通の暗号鍵及び復号鍵を作るため、大きな桁数の素数からこの共通鍵を作成する場合でも、各人毎にそれを行う必要がないため、多数の人数分の鍵を短時間で作成することができる。しかも、この共通の鍵は、個別の識別子又は個別の鍵と共にICカードに書込まれるので、ICカードで署名を作成する際には、共通の鍵と個別の識別子又は個別の鍵とを組合せて用いることにより、各人にユニークな署名を作成でき、よって、署名としての機能が十分に果たせる。尚、個別の識別子や個別の鍵の作成作業については、識別子のそれは単に異なるコードを決めるだけであり、個別の鍵のそれは桁数の少ない素数から作るものであるため、いずれも短時間で行える。

【0015】ICカード内では、秘密鍵としての復号鍵は、ICカードの書換え不可かつ外部読み出し不可の記憶エリアに記憶されることが望ましい。それにより、署名を他者が偽造することが不可能となりセキュリティが確保される。

【0016】本発明の第3又は第4の側面に従うICカードでは、記憶している秘密鍵たる復号鍵と識別子の双方を用いて、又は記憶している複数個の復号鍵を用いて対象情報を暗号化して署名を作成する。そのため、記憶している復号鍵と識別子とのセット、又は複数個の復号鍵のセットがそのICカードにユニークでありさえすれば、記憶している復号鍵の内の少なくとも1つが他のICカードと共通であっても、当該ICカードにユニークな署名を作成することが可能である。その結果、複数署

5

名者に共通の鍵を用いることが可能となるので、ICカード発行元において鍵を予め作成する処理時間が短縮され、多数人に対してICカード発行することが容易になる。

【0017】

【実施例】以下、図面を参照して本発明の実施例を説明する。図1は本発明を適用したデジタル署名システムの一実施例の全体構成を示す。

【0018】図1において、鍵生成センタ1は、RSA暗号を用いて多数の顧客に対する鍵を生成し、それぞれの顧客の鍵をそれぞれの顧客用のICカードに書込む作業を行うものである。この鍵生成センタ1は、まず、所定人数(=N人)の顧客のグループに対して、10進100桁程度の大きい2個の素数P1、Q1を1対だけ作成し(ステップS11)、この素数P1、Q1に基づいて1対の暗号鍵E1と復号鍵D1を作成する(ステップS12)。次いで、鍵生成センタ1は、互いに異なる値をもつN個のカード識別子IDj(j=1~N)を作成する(ステップS13)。

【0019】こうして1対の暗号鍵E1と復号鍵D1と、N個のカード識別子IDj(j=1~N)とを用意すると、次に、鍵生成センタ1は、暗号鍵E1と復号鍵D1とカード固有のカード識別子IDjとを予め用意したN枚のICカード2-j(j=1~N)に書込む(ステップS14)。

【0020】ここで、一般にICカードは周知のように、プログラムされたCPUとデータ等を格納する半導体メモリとを内蔵したICチップを有しており、半導体メモリ内の任意の記憶エリアに対し書き換え不可、読み出し不可(=ICチップ外への読出し不可)等の種々のアクセス規制を施すようプログラムされることができ、鍵生成センタ1に用意された各ICカード2-jは、署名実行プログラムがその書き換え不可エリア21に予め格納されている。そして、鍵生成センタ1は、上記復号鍵D1を秘密鍵として各ICカード2-jの書き換え不可及び読み出し不可のエリア22に、そのカード固有のカード識別子IDjを書換え不可エリア23に、また、上記暗号鍵E1を公開鍵として書き換え不可エリア24に書き込む。

【0021】このようにして、鍵生成センタ1は、所定のN人の顧客に対して、共通の暗号鍵E1と復号鍵D1と個別のカード識別子IDjとを書込んだICカードICカード2-j(j=1~N)を発行する。その後、鍵生成センタ1は、次のN人の顧客のグループに対し、前のグループとは異なる新たな2個の素数P2、Q2を1対作成し、これに基づき1対の暗号鍵E2と復号鍵D2を作成し、また、前のグループと同じN個のカード識別子IDj(j=1~N)を作成し、これらを新たなN枚のICカード2-j(j=N+1~2N)に書込んで発行する。以下、同様の処理を繰り返す。

6

【0022】以上のように、鍵生成センタ1は所定の複人数(N人)に対して1対の暗号鍵E1と復号鍵D1を割り当てるので、多数の人数分の鍵を短時間で作成することができる。また、発行されたICカード2-jでは、秘密鍵(=署名鍵)としての復号鍵D1が書換え不可及び読み出し不可のエリアに格納されているため、鍵生成センタ1以外の者がそのICカードを偽造することはできない。

【0023】図2は、本実施例において顧客がICカードを用いてデジタル署名を行う場合の処理流れを示す。

【0024】顧客が商品購入等の取引を行った際、顧客所持のICカード2-nが所定のカード用端末装置(図示せず)にセットされる。すると、ICカード2-nは、図2に示すように署名実行プログラムに従って、まず、端末から取引内容を記述した対象情報30を取り込み(ステップS15)、この対象情報30にカード識別子IDnを付加し(ステップS16)、この対象情報30とカード識別子IDnのセットを復号鍵D1で暗号化することによりデジタル署名31を作成して、この署名31を上記セットに付加する(ステップS17)。こうして作成された対象情報30とカード識別子IDnとデジタル署名31のセットは、ICカード2-nから端末を通じて取引相手へ電子的に送信される。

【0025】図3は一例として電話ショッピングの場合のデジタル署名の処理形態を示す。

【0026】顧客40が通信回線41を介して商品販売者42に対して商品を注文し(ステップS21)、商品販売者42が購入内容を示す情報43を顧客40に送信する(ステップS22)。顧客40はその購入内容情報43を確認した後、自己のICカード2-nを用いてその購入内容情報43に自己のカード識別子IDnを付加し、購入内容情報43とカード識別子IDnのセットを秘密鍵たる復号鍵D1で暗号化することによりデジタル署名44を作成し、このデジタル署名44を購入内容情報43と識別子IDnとのセットに付加し(ステップS23)、そして、この署名を付加した情報を商品販売者42に返信する(ステップS24)。商品販売者42は、返信された情報を購入内容情報43、識別子IDn及び署名44に分離した上で、署名44を公開鍵たる暗号鍵E1で復号化することにより元の購入内容情報43と識別子IDnを復元し、この復元した購入内容情報43と識別子IDnとを返信されたそれと照合することにより、正しい署名か否かを検証する。正しい署名であることが確認できると、商品販売者42は購入内容情報43を保管し、そして商品を顧客に配送する(ステップS25)。

【0027】以上のように、N人の顧客に秘密鍵(=署名鍵)として共通の復号鍵D1を付与していても、複合鍵D1とカード識別子IDnとのセットは各顧客にユニークであるために、カード識別子IDnと復号鍵D1と

7

を用いてデジタル署名を行うことにより、デジタル署名は各顧客にユニークなものとなり署名としての機能を果たすことができる。しかも、秘密鍵(=署名鍵)たる復号鍵D1は、書き換えもICチップ外への読出しも不可能であるため、署名の偽造は不可能であり署名の信頼性が確保される。

【0028】次に、図4及び図5を参照して本発明の第2の実施例を説明する。図4は第2の実施例の全体の構成を示し、図5はICカードによりデジタル署名を行う場合の処理流れを示す。

【0029】図4に示すように、鍵生成センタ50は、まず、前実施例と同様に所定のN人の顧客のグループに対し、10進100桁程度の大桁数の2個の素数P1、Q1を1対作成し(ステップS31)、これに基づき1対の暗号鍵E1と復号鍵D1を作成し(ステップS32)、次いで、N個のカード識別子IDj(j=1~N)を作成する(ステップS33)。次に、上記素数P1、Q1より桁数が少ない2個の素数pj、qjをN対作成し(ステップS34)、それらに基づきN対の暗号鍵ejと復号鍵djを作成する(ステップS35)。そして、N枚のICカード51-j(j=1~N)に、上記共通の暗号鍵E1及び復号鍵D1と、上記個別のカード識別子IDj、暗号鍵ej及び復号鍵djとをそれぞれ書込んで(ステップS36)、上記N人の顧客にそれぞれ発行する。

【0030】この後、鍵生成センタ50は、次のN人の顧客のグループに対し、別の新たな大桁数の素数P2、Q2を作成して1対の暗号鍵E2と復号鍵D2を作成し、この暗号鍵E2及び復号鍵D2と、前の顧客グループと同じ個別のカード識別子IDj、暗号鍵ej及び復号鍵djとを、次のN枚のICカード51-j(j=N+1~2N)に書込んで発行する。以下、同様の処理を繰り返す。

【0031】この実施例では、N対の暗号鍵ej及び復号鍵djを生成するが、その素となる素数pj、qjの桁数が少ないので、比較的短時間で生成することができる。

【0032】各ICカード51-jでは、署名実行プログラムが書換え不可エリア52に、共通の復号鍵D1が秘密鍵(=署名鍵)として書換え不可・読み出し不可エリア53に、個別のカード識別子IDjが書換え不可エリア54に、共通の暗号鍵E1が公開鍵(=検証鍵)として書換え不可エリア55に、個別の復号鍵djが秘密鍵(=署名鍵)として書き換え不可・読み出し不可エリア56に、個別の暗号鍵ejが公開鍵(=検証鍵)とし

8

て書換え不可エリア47にそれぞれ格納される。

【0033】顧客が自己のICカード51-nを用いてデジタル署名を行う場合には、図5に示すように署名実行プログラムに従い、まず対象情報60を端末から取り込み(ステップS37)、この対象情報60を共通の復号鍵D1で暗号化して第1の署名61を作成して、この第1の署名61を対象情報60に付加し(ステップS38)、更に、対象情報60と署名61のセットを個別の復号鍵djで暗号化して第2の署名62を作成して、この第2の署名62を更に付加する(ステップS39)。こうして作成された対象情報60と署名61と第2の署名62のセットが、ICカード51-nから端末を通じて取引相手に送信される。

【0034】この第2の実施例によれば、複数人に対し、比較的大きな桁数の素数P1、Q1に基づいて共通の1対の暗号鍵E1と復号鍵D1を作成し、かつ比較的小さな桁数の素数pj、qjに基づいて個別の暗号鍵ejと復号鍵djを作成して割り当てるので、従来例のように大きな桁数の素数Pj、Qjに基づいて個別の暗号鍵Ejと復号鍵Djを作成する場合に比較し短時間で鍵を作成できると共に、個別の鍵を用いない前の実施例より一層高いセキュリティを確保することができる。

【0035】

【発明の効果】以上説明したように本発明によれば、多数の人数分の鍵を短時間で作成することができるので、多数人を対象とするデジタル署名システムの実現に貢献できる。

【図面の簡単な説明】

【図1】本発明を適用したデジタル署名システムの一実施例の構成を示すブロック図である。

【図2】同実施例においてICカードによりデジタル署名を行う場合の処理流れを示すフローチャートである。

【図3】同実施例を用いて電話ショッピングで署名を行う場合の処理流れを示すフローチャートである。

【図4】本発明の第2の実施例の構成を示すブロック図である。

【図5】この第2実施例においてICカードによりデジタル署名を行う場合の処理流れを示すフローチャートである。

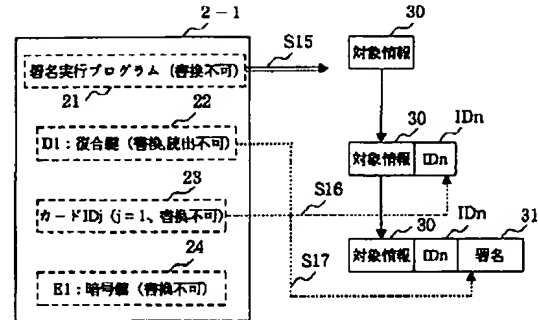
【図6】従来のデジタル署名方式を示すブロック図である。

【符号の説明】

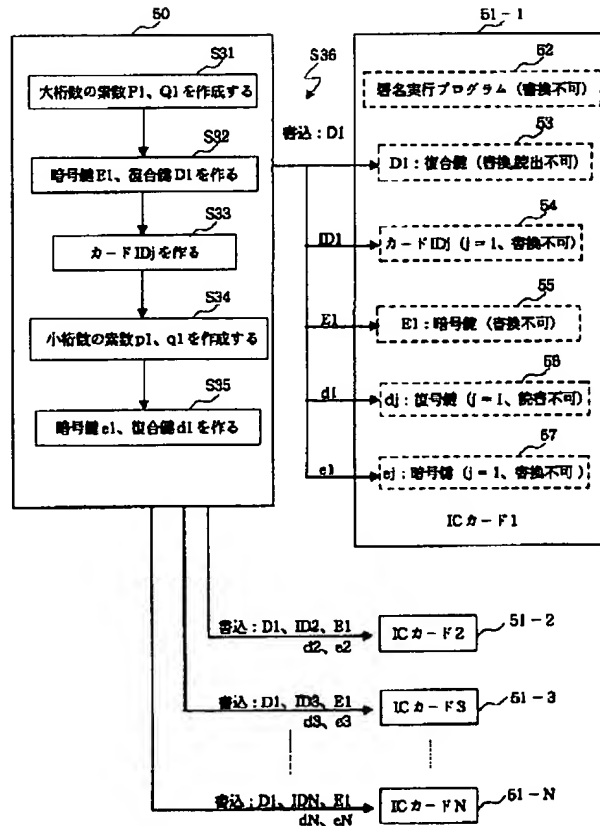
1、50 鍵生成センタ

2、51 ICカード

【図2】

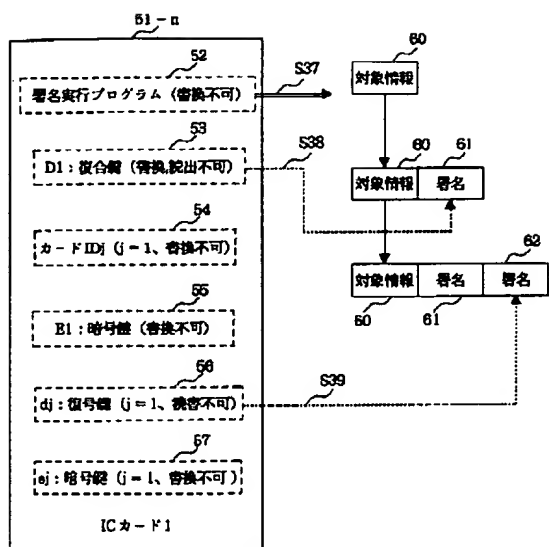


【図 4】





【図5】



【図6】

